The U.S. Navy's Vision for Information Dominance

May 2010

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The U.S. Navy's Vision for Information Dominance	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of the Navy,Chief of Naval Operations for Information Dominance,Washington,DC,20301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**22**	

Table of Contents

Foreword

The CNO has directed that the Navy position itself to remain pre-eminent in the fields of Intelligence, Cyber Warfare, Command and Control, Electronic Warfare and Battle & Knowledge Management. There is no other Service or nation that is as good, collectively, across these mission areas as the U.S. Navy. To obtain information age dominance, we will exploit new opportunities in distributed command and control, networking, and use of vast stores of collected data -- information and intelligence that too often lies at rest, undiscovered, unavailable, and untapped. In short, information will be elevated to a "main battery" of the U.S. Navy's arsenal. This paper provides a vision, principles, and initial direction to help guide us towards achieving our aspirations.

The concepts in this paper boldly point to the new niche Navy will fill at the intersection of maritime, information, and cyberspace domains. We do not seek to replace kinetic combat with information warfare or diminish the need for traditional instruments of military power. Rather, we aim to develop a penetrating understanding of our adversaries and an unmatched knowledge of the operating environment to amplify traditional naval combat capabilities and expand options for our operational commanders. As we develop a globally-distributed, highly networked force, our Fleet will become much greater than the sum of its individual parts. Fundamentally, our information capabilities are being designed to deliver game-changing decision superiority and command and control overmatch.

Time is short and the task paramount. Potential adversaries are working to offset our strengths and level the playing field. We can no longer afford inefficiencies incurred with stove-piped networks, systems and processes. Unless we leap ahead to develop a rigorous and comprehensive approach to control the electromagnetic spectrum and cyberspace, we will risk losing our competitive advantage. To achieve our aspirations, we must dramatically alter the status quo. The CNO expects us to develop and maintain a fleet battle management capability that synchronizes all elements of information, dominates the electromagnetic spectrum, and permits the Navy and our nation to wield information as a weapon.

I ask for your help in translating this vision into reality…

David J. Dorsett
Vice Admiral, U.S. Navy
Deputy Chief of Naval Operations
for Information Dominance

Vision

Pioneer, field and employ game-changing capabilities to ensure Information Dominance over adversaries and Decision Superiority for commanders, operational forces and the nation.

Purpose

To foster a forward-looking view of information as a core warfighting capability of the U.S. Navy. This paper begins the translation of information dominance from a vision into a set of concepts that will be tied with strategies and architectures in a series of Roadmaps. These Roadmaps will guide the Navy's future budgets, acquisitions and operational employment of information capabilities. The scope is Navy-wide with direct linkage to the other Sea Services and Joint and allied maritime operations.

Background

We have entered a new era. Globalization and the exponential growth in computing and communications capabilities have transformed the information environment from an enabling medium to a core element of warfighting capability, for both the U.S. Navy and our adversaries. Those adversaries, particularly al Qaeda and the Taliban, have skillfully applied information operations to achieve a temporary, asymmetric , tactical advantage, imposing tactical, if not strategic costs on US and coalition forces. Potential state and non-state adversaries are investing in capabilities to fight in the information domain and hold at risk our network dependent command and control capability. Indeed, on a daily basis, our nation's cyber networks are being relentlessly assaulted. Some even argue that we are already in the early phases of what will be a prolonged cyber war.

> **"Our technological advantage is a key to America's military dominance. But our defense and military networks are under constant attack. .... Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer -- a weapon of mass disruption. ... it's now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation."**
>
> 
>
> **President Barack Obama, 29 May 2009**

While the nature of warfare will endure, warfare modes are evolving to fit the unique characteristics of information age power, competition and conflict. Information technology and advanced warfighting concepts are creating new opportunities to enhance Navy's contribution to national security. To date, the role of information within Navy has been grown, despite the lack of an overarching conceptual framework and guiding principles. We have invested in superb sensors, weapons and control systems, but sub-optimized their combat effectiveness by designing them for and "welding" them to single platform types and individual units. This legacy platform-centric approach to capability and force development unacceptably increases our operational risk. In too many cases, our kill chain architectures cannot deliver data end-to-end.

"What all these potential adversaries -- from terrorist cells to rogue nations to rising powers -- have in common is that they have learned that it is unwise to confront the United States directly on conventional military terms. The United States cannot take its current dominance for granted and needs to invest in the programs, platforms, and personnel that will ensure that dominance's persistence."

SECDEF Robert M. Gates, January 2009

We have the means to redress these gaps and the attendant operational risk. Reiterating CNO guidance, ***"Aligning intelligence and operations and optimizing the network in many ways takes priority over the platform. If we don't get the intelligence and information right, then the platform is sub-optimized. Therefore, we need to elevate the priority of the information. ... Since we already think and operate this way, it's time we finally aligned organizationally to sustain it.... to achieve prominence and dominance."*** The U.S. Navy will decouple – programmatically and functionally – its platform-sensor-processor-weapon artifacts to reconfigure them as distributed, adaptively networked enterprise capabilities.

Navy's information capabilities will evolve from 20th century supporting functions to a main battery of 21st century American seapower. To be successful at 21st century warfare, the Navy will create a fully integrated C2, information, intelligence, cyberspace, environmental awareness, and networks operations capability and wield it as a weapon and instrument of influence. Information will be treated as a weapon across the full range of military operations. The transition to an information-centric Navy represents a new vision of who we are as a sea power.

Information Dominance – the Concept

Information Dominance is the ability to seize and control the information domain "high ground" when, where and however required for decisive competitive advantage across the range of Navy missions. Information Dominance means freedom of action to maneuver and act -- conduct offensive and defensive actions, kinetically and non-kinetically -- at the intersection of maritime, information and cyberspace domains. At this intersection, Navy exploits deep penetration, expanded maneuver space and information advantage to deliver warfighting options and effects. To achieve information dominance, the Navy must radically realign our warfighting capabilities. We must transition from a Navy that relies on individual units managing their own electromagnetic spectrum, to fleets and battle forces collectively achieving command and control over the electromagnetic spectrum in an automated fashion. This will require us to re-engineer our Navy – our concepts, our weapons, our battle management systems, and our people.

"The biggest breakthrough of the current fight in OEF and OIF is the successful integration of intelligence with operations, and using the network to get information to the right person, at the right time, in the right way. That is where the power is."
CNO ADM Gary Roughead, 17 July 2009

Information is no longer limited to an enabling role -- Navy information in warfare amplifies kinetic combat capabilities; Navy information as warfare delivers expanded maneuver space, new operational and strategic options, asymmetric operational effects, and capability for dominant control of the battlespace. Information as a weapon will be applied to influence, deny, degrade, disrupt or destroy across the full range of maritime and naval missions.

Assumptions

- Strategic competitors and potential adversaries are working to wrest the asymmetric advantage of Information Dominance to offset our strengths.
- In the future operating environment, commanders will continue to demand assured access to the right information at the right time.

- Strategic and operational C2 of a globally-distributed force requires new IT tools to achieve requisite levels of warning, situational awareness and insight.
- Remotely piloted, unattended and autonomous systems adaptively networked will increasingly populate and dominate the operating environment.
- Deep penetration and persistent monitoring of adversary networks for shaping of cyberspace will become a fundamental component of Navy operations.
- Navy cyberspace operations will mature rapidly to become a core component of theater forcible entry operations.
- Fiscal constraints will induce replacement of materiel and manpower with less costly information resources in non-traditional ways.
- Posturing Navy for strategic information advantage will also require new investments.

Information as a Weapon

This Navy concept for information dominance and decision superiority encompasses and links four interrelated meanings of the idea of information in warfare and as a "main battery" weapon:

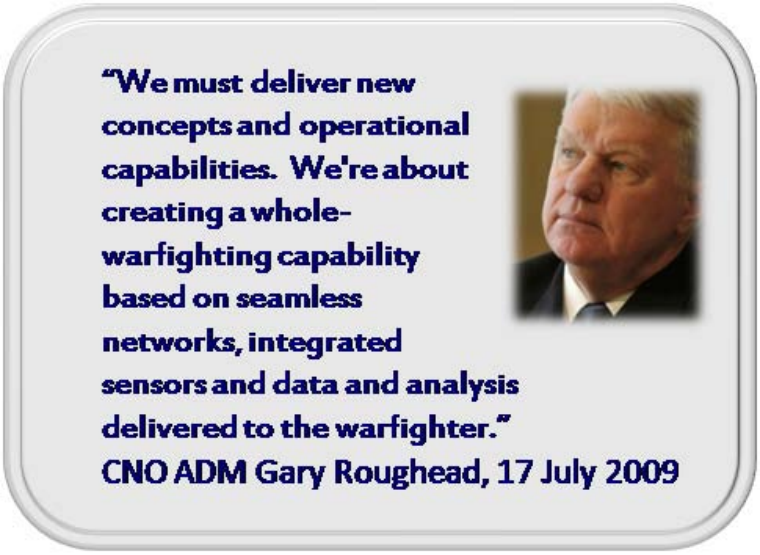
1. **Leap-ahead network and information integration capability**. A Navy that takes full advantage of advanced IT and network capabilities, enterprise data management, and all relevant data sources more agilely than the adversary. The objective is accomplished through two vectors -- 1) standards-based enterprise architecture integration; and 2) decoupling and re-integration of platform, sensor, processor, application, and data sets to resolve existing constraints (size, weight, power, net-centricity) and enable adaptive interface of all components via the network.
2. **Global enterprise net-centric operations.** Global-scale, adaptive netting of all Navy force and capability nodes to enable operation of the whole as a single, globally-distributed organism with no necessary differentiation between afloat, ashore, space, and cyber nodes nor between forward and rear nodes. Aggregate information power capabilities of Navy and external partners are brought to bear dynamically as the campaign or operation unfolds. All nodes are harmonized and in synch -- operating with access to the same information, awareness, direction, and controls for operational planning and execution.

3. **Information advantage overmatch in C2 and decision-making.** Optimally presenting data, information, intelligence, insight and knowledge such that the commander can make operational decisions and direct forces with such skill, rapidity, and effectiveness that the adversary cannot respond appropriately or in time to achieve his effects. Net-centric C2 capability to effect centralized direction and decentralized decision-making and execution is rendered far more dynamic and adaptive.

4. **Information power applied as the prime operational instrument.** Navy information power and purposeful control of the information domain achieved by 1) elevating use of information dramatically vis-à-vis traditional weapons (i.e., as first resort rather than an afterthought or firewalled "behind the green door" operation); 2) eliminating barriers to information integration (e.g., barriers between SCI compartments and SAP/IJSTO programs) to allow coherent application of all information capabilities and data resources; and 3) close integration of information warfare methods and TTPs with kinetic and non-kinetic warfare modes. Employment of information to exert control and achieve an operational effect at the time and locus of our choosing gives rise to information used as a weapon *per se* targeted for counter-platform, counter-network, counter-database, or counter-mind impact and influence.

Implications for Navy Operations in the Information Domain

The U.S. Navy will increasingly operate and maneuver in and through the information and cyberspace domains to achieve operational effects supporting naval missions and the national security. This paper creates a framework for achieving information dominance and decision superiority for commanders and operating forces. Key implications include:



- The currency of power in the Information Age is changed. Navy will adapt warfare modes to fit unique characteristics of Information Age power, competition, and conflict.
- Navy will align its strategic role, organization, and architecture to enhance both employment of information in warfare and information as warfare. Navy must accelerate information-based warfare modes and capabilities while retaining unparalleled ability to conduct traditional and hybrid warfare.

- Navy will place information on par with platforms, elevating information to status as a "main battery" of 21st century American seapower.
- Transforming information into a weapon requires deep penetration, awareness and understanding of the operating environment, of military, commercial, and social networks, of the mind of competitors and adversaries and of the "customer" -- a commander, decision maker, operator, analyst, or even a weapon.
- Net-centric operations provide new avenues for attaining deep penetration required to discern patterns of behavior, perceptions, and intentions and deep understanding of the environment.
- We will attain increased capability and decision superiority for our commanders and operating forces. The goal is assuring the warfighter get the right information at the right time to effectively perceive, understand, reason, decide, and command.
- This transformation imperative is about Navy's identity -- defining who we are and how we will adapt to meet new challenges and better support the national security. Navy is already an information warfare leader and will develop a strategy and plan for full-spectrum information power overmatch capability.
- We will increasingly rely on netted ISR capabilities and platforms, increasingly unmanned, that carry are multi-role sensors and collectors.
- Navy's Information Dominance Corps professionals, in junior grades, will be required to strengthen and deepen their professional skills in their communities and sub-specializations, while also obtaining a broader understanding of cross-Corps disciplines. Senior officers within the Information Dominance Corps will be required to broaden their professional expertise, and a growing number of senior officers will be assigned to cross-Corps assignments.

Guiding Principles

- **Every platform will sense and report** via the network -- Every Navy platform, no matter its geo-location will function as a data and information collector with responsibility for making information immediately available for use by other nodes.
- **Every sensor and processor will be adaptively connected** to the network -- Every entity is connected or on-demand connectable via standard interfaces in order to cross-cue and make local data and information globally available.

- **Collectors and sensors will be dynamically tasked and managed** over the global network-- collection and sensor management disciplines, processes and operations will be merged. Adaptive network reconfiguration will allow for either highly centralized or highly decentralized collector/sensor management modes.
- **Every shooter and weapon will be capable of compiling, assessing, exploiting and using composite target data from any collector, sensor or data repository** -- All data will be transported and ingested via a scaled up, enterprise-wide Cooperative Engagement Capability (CEC)-like tier of the global network architecture.

- **Data processing, correlation, exploitation, fusion and analysis will be network-hosted** for enterprise level dynamic management and load balancing -- Data will be hosted and used wherever optimal for the mission and conditions -- onboard, on the network, and at remote reach-back fusion nodes.
- **Remotely piloted, autonomous and unattended platforms and sensing and communication node capabilities will be emphasized** -- These capabilities facilitate penetration of and persistence in denied areas and help offset size, weight, power, and risk constraints associated with manned and tethered systems.
- **Globally-integrated, service-oriented backbone architecture** will be implemented with **scalable enterprise-wide services** -- The unified net-centric service-oriented, modular enterprise architecture will be designed around a common cloud (distributed peering network) with attributes such as on-demand services, customizable/user-defined interfaces, easy discovery, access and exploitation of data, and enterprise-wide security management. Applications will be rapidly developed and deployed to bring information warfighting advantage to bear in response to changing threats and opportunities in the operational environment.
- **Any sensor, data link, terminal or processor system that currently supports only one model platform or weapon will be migrated to the globally interconnected net-centric architecture or divested** -- Unintentional enterprise sub-optimization resulting from stove-piped solutions that benefit only a single element of the force will be eliminated.
- **All data and information will be rendered universally discoverable, transparent and accessible; data will be standardized across Navy and the maritime domain** -- Information is made available to all to decrease decision cycle times and enhance decision quality. A comprehensive and dynamic data strategy will drive efficient use of data bases and distribution of enterprise data fabric.

- **Joint, Defense, interagency, Intelligence Community partner architectures and data resources will be aggressively leveraged** in support of Navy missions and operations -- Navy will not duplicate investment in networks, infrastructure nor data resources that can be leveraged within the InfoSphere commons.
- **Vulnerabilities and risks uniquely associated with net-centric operations** will be rigorously accounted for, assessed and mitigated – Net-unique threat paths and potential cascading failure mechanisms will be accounted for and defended against.
- **Navy information professionals will receive world-class training, qualification, experience and tools**, and be expected to become prominent elements of Navy's warfighting arsenal.

The Information Dominance Corps

The CNO has directed that the Navy be the most prominent and dominant Service in the areas of Intelligence, Cyber Warfare, Command and Control, Electronic Warfare, Battle Management and Knowledge of the Maritime Environment. This aspiration is only possible if we continue to break down barriers between fields, professions and skills … and create a dramatically more competent and influential information-focused work force for the future.

Industrial Age organizations, processes and mindsets restrict our freedom of maneuver in the Information Age. Across the Navy, there has been unnecessary tension, duplication of effort, stove-piping, and lack of cohesion in how we acquire, manage and employ our networks, our intelligence, our cyber warfare and our command and control capabilities.

The creative transformation that the CNO has directed is analogous to the powerful revolutions in naval affairs that occurred when the Navy shifted from sail to steam, and from cruisers to dreadnaughts, or when we introduced naval aviation and nuclear power into the fleet. Comparable to past revolutions, the old order is being supplanted by new structures and processes. This revolution demands new thinking.

Unlike many past transformations, today's transition is not centered in the introduction of new platforms; but on positioning our Navy to achieve information dominance over potential adversaries and decision superiority for our commanders. Like Admiral Rickover and his talented team 60 years ago, we must champion innovation. In the lat e40s/early 50s, that innovation lead to the development of nuclear power, and advances in submarine design and operations. Today, our challenge is to deliver capabilities for the Navy that enable us to dominate across the information domain. We must take bold steps into an uncertain future.

In creating the Information Dominance Corps, CNO took a bold step in defining the Navy's future. Rather than accept a sub-optimal, rear-looking arrangement, where Navy's various "information" communities maintained separate and distinct roadmaps for their future, the CNO created a new structure that would optimize management of "information" professionals, and create new opportunities to collectively employ this extremely valuable element of the Navy's work force. By the simple act of creating a 45,000 person strong Corps, the CNO has better harnessed this "main battery" of his Navy.

For the near term, the CNO expects to dramatically increase the depth of professional skills of the members of the Information Dominance Corps. Navy's Information Dominance Corps professionals, in junior grades, will be required to strengthen and deepen their professional skills in their communities and sub-specializations, while also obtaining a broader understanding of cross-Corps disciplines. Senior enlisted, officers and civilians within the Information Dominance Corps will be required to retain depth in specialty and sub-specialty areas, while broadening their professional expertise across the information disciplines.

The Navy's leadership is looking to create a set of senior professionals who will become increasingly capable of managing and leading across the information domain. This will require some alterations to education, training and career paths. The fundamentals will remain the same, but the Navy will be placing greater demands on its Information Dominance Corps senior leaders. Indeed, expanding one's knowledge and skill is at the very foundation of what it means to become an information dominance professional.

Does the creation of the Corps mean communities are being subsumed? No. The Navy has benefited from the strength of its oceanography/meteorology, information professional, information warfare, naval intelligence communities and the space cadre. The creation of the Corps should serve to reinforce the value of the communities, while creating a mechanism for the Corps to become much more than the sum of its individual communities.

Navy Information Dominance Roadmaps

A series of "Roadmaps" will be created as a mechanism to jumpstart information dominance initiatives, and align activities. These roadmaps are being crafted to synchronize commands and activities, across the Navy, who are responsible for achieving the CNO's vision. The roadmaps, which will focus on information-focused areas, will provide guidance regarding the concepts, architectures, networks, sensors, manpower, and platforms required to achieve dominance in each respective mission area. They are information-centric, vice platform-centric guides.

Over the next 18 months, the Navy will create the following Roadmaps:

- **Air Dominance**: Define the way ahead for "informationizing" Navy operations conducted throughout an integrated aerospace domain.
- **Converge to a Single Navy Network**: The Navy's approach for achieving a single integrated network environment that allows Navy users and assets to seamlessly access and share classified and unclassified information globally in performing their missions.
- **Cyberspace Operations**: Create an agile, cost efficient approach to facilitate information dominance, non-kinetic advantage and kinetic superiority through dynamic creation, utilization and defense of data, information and networks.
- **Decision Superiority**: Close the raw data to information to knowledge cycle in a manner to deliver the commander a capability that makes every option available every time in every level of warfare.
- **Education**: Broaden and deepen skill sets and create world-class expertise across the Information Dominance Corps through investment in educating and training.
- **Electromagnetic Spectrum Management**: Develop a profound understanding of the electronic environment to allow for freedom of information exchange in any communications situation, while making adversary usage of the same environment his greatest challenge.
- **Fleet Battle Management**: Derive a process and architecture that allows for optimal employment of resources. Include the ability to support C2 from the location that best meets mission needs, is responsive to changes in the operating environment and maintains commander's intent.
- **Integrated Surface Sensors**: Network disparate sensor, data transport/exchange, processing, visualization and decision support capabilities afloat for horizontal integration.
- **Intelligence, Surveillance, and Reconnaissance**: Focus on enabling decision superiority through our ability to transform raw data to information and information to knowledge.

- **Maritime Ballistic Missile Defense**: Use information better and in different ways to enable the Phased Adaptive Approach (PAA) and improve holistic BMD capability across all phases of operations.
- **Maritime Domain Awareness**: Significantly advance the Commander's Decision Superiority by bringing together intelligence, information and networks and leveraging prior investments, technologies and IC efforts.
- **Spectrum Usage**: Leverage the benefits inherent to Navy capabilities and doctrine to the maximum technical feasibility to deliver ensured communications that are optimized in both access and cost. Deny our adversaries like capabilities.
- **Strike Command and Control**: Define the manner in which we employ and transfer information to enable Navy to fully realize strike platform competitive advantage against any adversary.
- **Undersea Dominance**: Align and network capabilities to achieve Undersea Information Dominance across fixed, mobile, manned and unmanned.
- **Unmanned Systems**: Achieve integration and synchronization among manned and unmanned systems, and unattended sensors, and across all domains (air, surface, subsurface, and shore).

Game Plan: Near Term Priorities/Objectives

Organizational Alignment:

- Institutionalize the DCNO for Information Dominance (OPNAV N2/N6) – evolve the structures and processes required to define, develop, resource and oversee the Navy's information capabilities.
- Mature Fleet Cyber Command (US Tenth Fleet) as the Naval Component Commander for USCYBERCOM; present USCYBERCOM and USSTRATCOM with world-class Service component cyber forces to lead in defining the future of cyberspace operations.
- Develop CYBERFORCOM and COMNAVMETOCOM as the Type Commanders for the Information Dominance Corp and aggressively improve man, train, equip (MTE) functions across the information domain.
- Refocus NETWARCOM mission for excellence in NetOps and Space Operations.
- Engage key national and joint space-related entities to ensure current and future Navy needs in space are identified, understood, and resourced.

- Align oversight, governance and synchronization mechanisms to deliver end-to-end insight and accountability for Navy information requirements, investments, capability development, and force development.
- Coordinate information dominance efforts, including Science and Technology efforts, across DoD, interagency and international partners.
- Implement processes that synchronize warfighting gaps, identify solutions, and align investments within the PPBE timeline, culminating in holistic warfighting capability investments.
- Examine improved information requirements to capability acquisition governance/processes to better align Moore's Law and the lengthy PPBE/JCIDS process.
- Develop a series of Roadmaps that will guide Navy development of its future Information Dominance capabilities.

Our People:

- Establish the Information Dominance Corps with the lead role in an innovation campaign; develop a strategy to strengthen community professionalization, cross-qualify, identify and resolve barriers and boundaries between information disciplines and programs. Build tighter linkage between all IDC communities and warfare operators for decision superiority.
- Establish an IDC basic school for all navy enlisted classification codes, officer designators, and civilian job series comprising the IDC, and establish specialized training to develop unique skill sets to meet billet requirements beyond the skills and knowledge that general ratings, designators, or series would provide; if impractical, consider adding IDC core competency "blocks" to basic schoolhouse training curricula.
- Establish an innovative training continuum utilizing cutting edge technologies and proven instructional techniques to provide the force with the "right people at the right time at the right place with the right skills" delivering a fully integrated corps of Information Dominance professionals that understand the consequences of their actions for better decision making.
- Posture the Navy Space Cadre to advocate for Navy requirements in the National/ DoD space decision making process. Develop policy/vision/strategy for continued development of the Space Cadre, including its enlisted and civilian membership. Identify a Space Cadre billet/position base that will ensure highly qualified Space Cadre members are placed where they can best advocate for Navy requirements.

- Our strategy, doctrine and resources should reflect the balance between unmanned and remoted sensors with scarce manpower and low density language/technical skills.
- Create and sustain "cyber-savvy" Navy Officers and Enlisted by adjusting and implementing the existing educational and training architectures, to include at a minimum: Navy Professional Education; Joint Professional Military Education; Maritime Advanced Warfare Courses; and the Fleet Training Continuum.
- Create a focused, high fidelity cyber Reserve force functionally interwoven with cutting edge cyber industry enabling a mutual beneficial exchange of cyber knowledge and best practices.

The Current Fleet:

- Ramp up efforts to acquire profound understanding of the maritime environment.
- Field enhanced intelligence, surveillance, reconnaissance and targeting processing and exploitation capabilities on large deck combatants, maritime operations centers, and training commands.
- Strengthen partnerships with allied coalition and interagency partners through federated network integration and increased maritime information sharing; promote new partnerships with international and industry maritime stakeholders.
- Encourage the development of regional maritime information sharing networks.
- Resolve cross system interoperability issues.
- Integrate IT21 networks acquisition, training, and logistic support requirements to enable the efficient and effective delivery of capability across interconnected programs to facilitate the Navy Network Enterprise.
- Transition from reactive to proactive computer network defense; improve technical and managerial measures designed to ensure the confidentiality, control, integrity, authenticity, availability and utility of information and information systems comprising ashore and afloat networks.
- Field the Navy's initial fleet of unmanned underwater vehicles.
- Deliver modern surface electronic warfare to the fleet through the surface electronic warfare improvement program and ship's signal exploitation equipment providing order of magnitude improvement in defensive capabilities and enabling distributed, networked, and integrated force electronic warfare.
- Increase investments to improve electronic warfare material conditions and develop expertise in electronic warfare and electromagnetic spectrum operations.

- Enhance capital planning and investment control process for cyber-related capabilities specifically intended to increase portfolio cost benefit ratios and mission performance to the highest levels.
- Continue refining/consolidating our understanding of existing Navy networks with thoughtful decision making of which should be consolidated and which should be isolated.

The Future Fleet:

- Our future depends on the ability to leverage emergent technologies to include unmanned and remoted sensors in all domains: land, sea, air and space. Develop plan for information dominance engineering and acquisition disciplines to support timely, affordable fielding and life cycle management of relevant enterprise services, information systems and information weapons.
- Develop Sea Trial experimentation strategy to hone information strengths and mitigate vulnerabilities associated with networks and net-centric operations.
- Leverage technologies that facilitate interoperability among currently fielded systems. Apply Sea Trial and TRIDENT WARRIOR to validate their military utility and quantify their return on investment.
- Accelerate Navy enterprise architecture integration and apply advanced information technology to enable unfettered information flow across the globally-distributed and netted Navy.
- Develop true multi-intelligence and information fusion and collaborative capabilities incorporating leap-ahead technology improvements in computing and advanced analytics.
- Develop a concept for the nexus between theater ballistic missile defense, space operations, cyberspace operations, and forward cyber security as a core Navy operating niche.
- Develop squadron of low observable unmanned combat aircraft capable of operating from aircraft carriers, and employing networked ISR sensors and precision guided munitions by 2018.
- Transition from current manned airborne SIGINT platforms to sea-based, unmanned, multi-intelligence capabilities – IOC sea-based medium-range multi-INT aircraft.
- Evolve fleet maritime operations centers as the central node for the operational level of war, maintaining awareness of each AOR and providing Commanders with improved information and intelligence for decision advantage.

- Define the future concepts of operations, collaborative concepts, and scalable network attributes required to dynamically execute missions and rapidly reconfigure warfighting assets to accommodate future operations (e.g., migrate to every platform a sensor, every sensor networked.)
- Introduce the E-2D and its advanced capabilities.
- Continue to develop and mature Joint interoperable sensor fusion capabilities, in line with collaborative engagement capability, to support ballistic missile defense as well as traditional air, sea and undersea warfare.
- Transition from legacy IT21 afloat networks to consolidated afloat networks and enterprise services to streamline acquisition, training and logistic requirements and to facilitate the necessary network infrastructure and services to ensure secure, adaptable and affordable network platform supporting multiple existing and evolving mission areas with fewer sailors.
- Develop a single integrated network and communications environment that allows Navy users and assets (sensors, systems, and applications) to seamlessly access and share information globally, ashore and afloat, in performing their missions.
- Develop and operate an information transport system that will provide for the timely delivery of critical command and control information, is interoperable with other service systems and is not susceptible to service denial efforts of dedicated enemy attack.

- Develop an integrated space-based earth observation remote sensing plan combining Navy unique requirements, inter-service and interagency joint mission opportunities, and exploitation of data from National sensors.
- Develop plans by 2015 to recapitalize the T-AGS fleet as a class of modular ships able to support ocean survey operations, unmanned system launch/recovery/husbanding operations, and other national missions.
- Develop and quickly field innovation knowledge generation capabilities through cross-discipline fusion and exploitation of the new information that will be available through networked battlespace awareness sensors.
- Recapitalize Navy's undersea surveillance capability.
- Develop fully distributed, integrated, networked, and automated force EW capability.

- Develop Force battle management system providing automated and integrated hard kill and soft kill coordination.
- Align Navy multi-INT collection and analysis nodes as contributors and consumers of National cloud-enabled data stores.
- Execute integrated kinetic and non-kinetic cyber warfare capabilities in support of Navy and combatant command operations while conducting global dynamic network defense operations.

The Ashore Infrastructure:

- Develop a path towards a more open architecture with data standards that address the needs of all maritime stakeholders (fleet, DoD, intel community, interagency and international partners) while maintaining the need for security in certain efforts.
- Centrally manage and consolidate common information technology services (portals, data centers, software licenses) across the Navy enterprise.
- Develop cyber reserve hubs collocated with industry cyber leaders to enable collaborative cross sharing of cyber capabilities and cyber tactics, techniques and procedures.

Caution

While building leap-ahead integrated network and enterprise-wide capabilities, we must monitor and mitigate specific vulnerabilities associated with increased reliance on net-centric warfare. Among these risks (but not all inclusive) are the danger of overspecialization and overreliance on information as a substitute for traditional factors, oversimplification of complex underlying realities and relationships, and overreliance on risk-management and operational net assessment models and battle simulations. In addition, while Navy advances information power capabilities and TTPs, complex policy, legal and ethical questions must be addressed up front. There are ways of war that will not be consonant with American values or that we will not want to encourage others to emulate. Finally, this concept does not aim at or promise to deliver paralyzing shock and awe, a transparent battlefield, elimination of all fog and friction, bloodless warfare, or warfare on the cheap. Rather, it aims to apply information resources smarter, in all operational dimensions, to make Navy the model of information warfighting prominence and dominance.

Summary

The opening salvos of the future conflict in cyberspace have already been fired. Like the Cold War, this will be a sustained conflict, involving not a single foe but multiple, sometimes anonymous adversaries. Violent extremist and terrorist movements, strategic competitors, regional adversaries, and even criminal elements are determined to erode our nation's preeminent information capabilities. Our challenge is to maintain a decisive information advantage over adversaries across an information-intensive, multi-domain operating environment that continues to expand daily in terms of its scope and complexity.

Navy, therefore, must cast off old structures and processes to exploit opportunities in the Information Age and sustain and extend our competitive advantage in the information domain. Achieving our vision of Navy Information Dominance requires that we eliminate long-standing institutional and functional barriers that impede the full integration of operations and information. We must also take a holistic approach to the development and integration of our sensors, networks, processes, and information professionals.

While much importance has been placed on the Cyber Domain, Success in the Information Age will also require unmatched mastery of the capabilities, tools and techniques that enable us to collect, process, analyze and apply information. With them, we develop an in-depth understanding of our adversaries and profound knowledge of the environments, both real and virtual, in which we operate. We therefore must invest in the unmanned capabilities required for persistent surveillance of the maritime environment. We must ensure our platforms are equipped with an integrated, networked, system of sensors to provide information that ranges from baseline situational awareness to deep penetration of adversarial capability and intent.

We must recruit, develop and retain a team of world class information professionals that will develop, manage, and employ our information-based capabilities. Network and cyber professionals to build, operate, defend and fight on our networks. Intelligence analysts and collectors with technical, language, and cultural expertise. Meteorologists and oceanographers to not only expand our knowledge of the maritime environment, but provide commanders with an understanding of the operational impacts of developments within that environment. Experts in space-based intelligence, communications, and sensing capabilities to lead the development and acquisition of the next generation of overhead constellations.

Success in competition and conflict will increasingly hinge on the speed and agility of our decision-making and C2. We must also overcome a historical resource investment bias that has favored cold steel over electrons, information, human cognitive, and command capacity. Information must become a main battery of the U.S. Navy, but the power of our aircraft, ships, submarines and our people is not to be ignored. Throughout history, warfare has been about both manipulating one's enemy, and when necessary, destroying that enemy. There is room for both Sun Tzu and von Clausewitz in the information age.

The promise of future strategic and operational capabilities arising out of information dominance and decision superiority is profound. The U.S. Navy stands on the cusp of a transformational revolution no less important to our warfighting preeminence than the transition from sail to steam, from battleships to carrier aviations, from fossil fuels to the introduction of nuclear power. The implications for our force structure and the operational employment of information-centric warfighting capabilities are equally profound, spanning all current mission areas. The Chief of Naval Operations has set a clear course for realigning Navy organizations to operationalize cyberspace and information operations by establishing FLTCYBERCOM/TENTHFLT and reorganizing the OPNAV Staff to achieve integration and to foster innovation. Information-centric functional integration, innovation and an end-to-end approach to development of unmanned and autonomous systems will deliver warfighting dominance across all domains. Our follow on strategy and roadmap will guide requirements, architecture and the procurement plan to attain Information Age operational capabilities.